Amendments to the Specification:

Please make the following amendments to the specification:

[0005] It is known to use an external storage device for a computer that uses a removable medium which can be attached to and detached from a system. A removable medium has been widespread in use in part because of its superior portability and also in part as the recording medium can be taken out of a storage device. Additionally, it is known that a removable medium also provides convenience to an end user in that it can be attached to a computer for immediate use. There are various kinds of removable media such as an ATA (AT Attachment or Advanced Technology Attachment) card to be used for a PCMCIA (Personal Computer Memory card International Association) slot, a USB (Universal Serial Bus) card to be attached to a USB port for use, and a magnetic disk or an optical disk to be mounted on a dedicated disk drive (driving device) for use.

[0036] As shown in FIG. 1, a computer used in an embodiment of the present invention is provided with a CPU 11 for performing various processing and controlling activities, a memory 12 used in a program for controlling the operation of the CPU (Central Processing Unit) 11 or in processing by the CPU 11, a PCMCIA controller 13 and a USB controller 14 for controlling an external storage device, and a video controller 15 and a display device 16 for displaying a user interface screen. The PCMCIA controller 13 is provided with a slot (PCMCIA connector) to which a PC (Personal Computer) card is mounted, and an ATA card, which is a removable medium, can be mounted to the slot as an external storage device. The USB controller 14 is provided with a USB connector, and a USB memory, which is a removable medium, can be mounted to the USB connector as an external storage device.

[0049] The encryption processing part 150 performs encryption and description of a data file. Standard algorithms such as RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5) and AES (Advanced Encryption Standard) can be used as an algorithm used for encryption and decryption. The encryption processing part 150 may be not only realized with software executed by the program-controlled CPU 11 as described above but also realized by a dedicated chip (hardware) with an encryption circuit included therein. The specific operation of encryption processing is further described hereinbelow.

[0070] As shown in FIG. 7, the encryption engine 151 inputs a passphrase and data to be encrypted, decrypts the data based on the passphrase, and outputs it (hereinafter, data encrypted by the encryption engine 151 is referred to as encrypted data, and encrypted data with predetermined header information added thereto is referred to as an encrypted file). Various algorithms such as RC2 (Rivest Cipher 2), RC4, RC6 (Rivest Cipher 6), 3DES (Triple Data Encryption Standard) and AES can be used as an encryption algorithm and they can be dynamically changed for application. By dynamically changing an encryption algorithm, security can be improved.

[0071] The hash value generation engine 152 inputs a passphrase and data to be encrypted, calculates a hash value of the data based on the passphrase and outputs it. As a hash function for calculating the hash value, MD5 (Message-Digest algorithm 5) can be used, for example.